IN THE SPECIFICATION:

Please replace paragraphs 16 and 18 with the following paragraphs annotated with changes made.

[0016] SoCs in general are familiar to those skilled in the pertinent art and thus will not be described in detail greater than necessary to convey the inventive concepts introduced herein. The SoC 100 includes a central processing unit (CPU) 110. The CPU 110 is coupled via buses (some of which are shown and designated 112, 114, 116) to various peripheral components. Among those peripheral components is a secure memory space 120 composed in the specific embodiment of FIGURE 1 of a secure read-only memory (ROM) 122 and secure static random-access memory (SRAM) 124. The CPU 110 has access to external memory 118 and other components (not shown) via the bus 112. Because it goes outside the SoC 100, the bus 112 requires various external pins (only one of which is designated 102) of the SoC 100. Thus, the CPU 110 and peripheral components can receive and transmit programs, data and control signals from and to the external memory 118 ~~116~~ and other external system components in a manner that is well known to those skilled in the pertinent art.

[0018] FIGURE 1 also illustrates a schematic representation of a hybrid cryptographic accelerator 140 constructed according to the principles of the present invention. The term "hybrid" is appropriately used because, as FIGURE 1 illustrates, the cryptographic accelerator 140 straddles both the SEE 130 and the portion of the SoC 100 that is outside of the SEE 130. More particularly, a key register 142 of the hybrid cryptographic accelerator 140 lies within the SEE 130 and is coupled to the secure ROM 122 and the secure SRAM 124 by a secure bus 116 ~~126~~. In contrast, data input and output registers 144, 146 of the hybrid cryptographic accelerator 140 lie outside of the SEE 130 and

are coupled to the CPU 110 by a bus 114 ~~112~~ that is not secure and therefore is wholly separate from the secure bus 116 ~~126~~. Thus, the hybrid cryptographic accelerator 140 operates partially within and partially without the SEE 130. As will be described below, this arrangement yields a particularly advantageous operation that accommodate both cryptographic key security and high data throughput.